Cassandra Crossing/ Globaleaks, oltre Wikileaks

(235)— Mentre Wikileaks combatte per la sua esistenza, c'è chi sta costruendo un futuro migliore per la "Public Disclosure"

Cassandra Crossing/ Globaleaks, oltre Wikileaks

Figure 1:

(235)— Mentre Wikileaks combatte per la sua esistenza, c'è chi sta costruendo un futuro migliore per la "Public Disclosure"

7 settembre 2011—Esistono moltissime persone che ritengono la pubblicazione di informazioni riservate (Public Disclosure), che in certi casi può anche avere effetti immediati negativi, un grande guadagno netto per la società civile.

Nella precedente categoria esistono tuttavia persone che hanno criticato da molti punti di vista Wikileaks, il suo funzionamento, e l'operato dei suoi rappresentanti (presenti e passati) più noti, in particolare Julian Assange e Daniel Domscheit-Berg.

Coloro che promuovono o facilitano pubblicamente le attività di Wikileaks ritengono evidentemente che esse siano benefiche e positive: sono nella maggior parte dei casi entità umane come dissidenti politici, cittadini che temono ritorsioni, attivisti dei diritti civili e semplici consumatori.

Le attività di Wikileaks sono invece solitamente poco apprezzate (per usare un eufemismo) da entità non umane come stati ed organizzazioni di vario tipo ed aziende.

In questo contesto è curioso che si parli così poco del lavoro di chi sta costruendo o tentando di costruire il futuro della "Public Disclosure": molti interessati al fenomeno ignorano del tutto che esistano evoluzioni anche molto significative.

L'argomento Public Disclosure in quanto tale è praticamente assente dai media: qualche notizia appare di tanto in tanto, ma si tratta di pezzi di pura cronaca su Wikileaks, sulla la

vicenda giudiziaria di Julian Assange o più recentemente sui cable pubblicati senza filtraggio da Wikileaks stessa.

Il povero Julian, non ce lo dimentichiamo, è ancora ai domiciliari nel Regno Unito ed attende la discussione della strumentale richiesta di estradizione svedese-americana che lo potrebbe portare in tre semplici passi a Guantanamo.

Si meriterebbe, è stato già scritto, di essere ricordato più spesso.

Ma oggi non parleremo di lui, di Wikileaks o della vicenda dei cablo non rieditati, ma piuttosto dei limiti e degli errori di realizzazione del "sistema" Wikileaks, e soprattutto delle attività di gruppi di persone che, imparando dalle lezioni del passato, cercano di fare qualcosa di migliore.

Per poter descrivere quello che c'è oltre Wikileaks, è necessario prima considerare che cosa è, e sopratutto che cosa non è, Wikileaks.Wikileaks è un'organizzazione centralizzata che vuole promuovere ed attuare Public Disclosure.

Non è una "entità di Rete" e nemmeno un software: questi sono in effetti i suoi maggiori limiti.

Wikileaks ha a che fare con la Rete solo perché nella maggioranza dei casi riceve documenti in forma digitale (come ormai accade in tutti i trasferimenti di informazioni), e perché utilizza principalmente ma non esclusivamente un sito web per propagandare se stessa e diffondere la maggior parte dei documenti.

Wikileaks ha dichiarato di permettere anche consegne telematiche via sistemi anonimi, come Tor, ma questa possibilità è stata spesso indisponibile. Esistono anche indirizzi postali e sicuramente altri mezzi convenzionali ma non completamente pubblici.Da questo punto di vista, quindi, Wikileaks cerca di mettere a disposizione di tutti la possibilità di rendere pubbliche informazioni utilizzando anche vari mezzi informatici senza tuttavia essere riuscita a farlo in maniera sicura: non per nulla si è praticamente bloccata appena qualche "peso massimo" si è reso conto di cosa stava succedendo.

Dal punto di vista della sicurezza di tutti i partecipanti al processo di Public Disclosure questi sono i punti deboli di Wikileaks:

1. [essere un'organizzazione centralizzata e pubblica, e quindi attaccabile e neutralizzabile anche se tenta di rendersi più resistente con accorgimenti come avere più server in paesi diversi od offuscare l'identità dei suoi collaboratori.]
2. [non garantire l'anonimato di chi fornisce le informazioni in maniera dimostrabile, ma solo su una base "fiduciaria".]
3. [non sfruttare la Rete e le sue potenzialità per rendere diretto ed automatico il processo di comunicazione tra chi fornisce le informazioni e chi le rende pubbliche]
4. [dover obbligatoriamente agire come filtro sulle informazioni e come decisore del Target, cioè facendosi carico di attività molto pesanti in termini non solo operativi ma anche di responsabilità, sia morale che giuridica.]

Alcune comunità di persone si sono rese contro che l'intero processo di Public Disclosure doveva essere ripensato e reso più sicuro e più semplice utilizzando mezzi informatici e la Rete, e che la cosa doveva essere realizzata proteggendo al massimo, particolarmente dal punto di vista delle responsabilità legali, tutti gli attori del processo.Il modello di anonimato forte e plausible deniability adottato da Freenet ne è un buon esempio.

Il primo tentativo, che ancora non ha prodotto un sistema utilizzabile, è quello di Openleaks, che è stato portato avanti principalmente da un ex membro di Wikileaks, Daniel Domscheit-Berg, che ha organizzato una community per creare una "Wikileaks come avrebbe dovuto essere".

Openleaks mette in comunicazione la persona che fa la Public Disclosure e il medium responsabile della pubblicazione, proteggendo in maniera dimostrabile l'anonimato di chi fa filtrare l'informazione riservata. È in buona sostanza una dropbox anonima da cui i giornali possono attingere notizie.

Questo risolverà, quando sarà realizzato e funzionante, la maggior parte dei problemi pratici da cui Wikileaks è afflitta.

Resta però da risolvere il problema più critico, la centralizzazione dell'organizzazione e l'accorpamento di ruoli che sono nella pratica ben distinti.

Openleaks, o una serie di siti come Openleaks, saranno sempre attaccabili e neutralizzabili con tecniche DoS di negazione del servizio, sia informatiche che legali, ma sopratutto sia legali che paralegali o addirittura illegali. Senza correggere quest'ultimo punto, Openleaks sarà in grado forse di proteggere i suoi utenti ma non se stessa.

Ed è questo ultimo indispensabile passo che Globaleaks ha realizzato, utilizzando estesamente come "mattoni" risorse per la privacy già disponibili, diffuse e ben collaudate come Tor, gli Hidden Services di Tor ed il proxy Tor2Web.

Globaleaks non è un'organizzazione, e nemmeno un gruppo di persone collegato in qualsiasi modo ai processi o ai siti di Public Disclosure: è una comunità di persone che sviluppa e mantiene, apertamente e su scala internazionale, una singola applicazione libera ed open source chiamata appunto Globaleaks, utilizzando Wiki e Launchpad.

I suoi membri, che, partecipando ad una comunità aperta e pubblica, non devono partecipare al processo di Public Disclosure (almeno non in maniera dimostrabile), hanno un identico ruolo, battezzato "Random Globaleaks Contributor", sia che sviluppino codice, documentazione, facciano test o semplice propaganda.

L'architettura di Globaleaks definisce chiaramente i ruoli nel processo di Public Disclosure, e li protegge nella massima misura possibile ottimizzando e rendendo automatico e flessibile l'intero processo.
Essa permette non solo di far uscire l'informazione in modo sicuro, ma anche di decidere chi sarà colui che la riceverà, tutelando per quanto possibile l'anonimato di tutti i ruoli.

Questa flessibilità permette di estendere l'applicazione della Public Disclosure dal semplice comunicare ai giornalisti la notizia fresca su cui scrivere il pezzo, all'utilizzo in campi quali dinamiche aziendali, attivismo politico e promozione della trasparenza.

GlobaLeaks infatti vuole soddisfare le esigenze di tutti questi attori che compogono il vasto ecosistema di quello che oggi viene indicato come "Whistleblowing", di cui i giornali e i media sono solo una piccola parte.

I ruoli definiti da Globaleaks sono quelli di "Administrator" (creatore e gestore di un nodo Globaleaks), di "Whisteblower" (chi fa uscire le informazioni riservate) e di "Target" (la persona che pubblicherà le informazioni).

Le caratteristiche principali di Globaleaks sono:

1) non esiste nessun sito centrale o ruolo che conosca tutte le informazioni di una Public Disclosure, e che possa essere colpito con mezzi legali od illegali.
2) l'intero processo di consegna è guidato da chi rischia di più, cioè dal Whisteblower.
3) esiste una molteplicità di piccoli "siti Globaleaks", anonimi ed irrintracciabili, creati in maniera semplice da chiunque voglia utilizzare il meccanismo della Public Disclosure per favorire chi desidera divulgare informazioni.

Questi siti, destinati a rimpiazzare Wikileaks, saranno molti, “piccoli” e specializzati su un certo argomento, territorio o soggetto.

Facciamo l’esempio di una persona preoccupata di un problema: lo smaltimento illegale di maleodoranti pannolini usati per bambini. Questa persona potrà decidere di creare un sito Globaleaks semplicemente installando, su un qualsiasi pc connesso alla Rete, una copia del software Globaleaks.

Il software, in maniera automatica ed utilizzando la rete Tor, creerà un Hidden Service Tor di tipo web.

Nascerà così un sito web tematico interno alla rete Tor e raggiungibile solo per mezzo di essa, e la persona assumerà il ruolo di “Administrator” di questo sito.

Come Administrator intitolerà il suo sito Globaleaks “Cittadini Preoccupati Dello Smaltimento Dei Pannolini Usati” ed al suo interno inserirà le indicazioni che ritiene utili per chi lo dovrà utilizzare per rendere pubbliche informazioni (questo secondo ruolo è chiamato “Whisteblower”), ed una lista di persone che l’Administrator giudica interessate a ricevere e pubblicare questo tipo di informazioni (questo ruolo è chiamato “Target”)’.

Renderà poi noto a chi ritiene opportuno, in maniera più o meno pubblica e con mezzi più o meno anonimi, l’indirizzo Tor, l’esistenza e lo scopo di questo sito. A questo punto il ruolo dell’Administrator, che comunque potrà monitorare quello che accade sul suo sito, può considerarsi esaurito.

Conoscendo l’esistenza del sito CPPLSDPU, una persona che vedesse il suo forzuto e permaloso vicino di casa interrare in giardino i pannolini usati del suo pargolo in totale disprezzo delle norme sanitarie, possedendo l’indirizzo Tor del sito “CPPLSDPU” potrà scattare una fotografia al vicino con la pala in mano, preparare un documento e tramite Tor (se lo sa utilizzare) o utilizzando un proxy Tor2Web (con meno privacy ma più semplicità) caricarlo sul sito CPPLSDPU, assumendo così il ruolo di Whisteblower.

In maniera automatica il sito crea un oggetto chiamato “Tulip” (“Tulipano”, vedremo poi il perché del nome) che contiene il documento, e ne fornisce la password di accesso al Whisteblower.

Il sito poi trasmette l’informazione sull’esistenza del Tulip e del documento in esso contenuto alla lista dei Target precedentemente definita dall’Administrator, insieme al link Tor necessario per scaricarlo.

Nella versione in sviluppo di Globaleaks per ora questo avviene via mail.

You are the Whistleblower

Figure 2:

Ogni Target, ricevendo la mail, potrà collegarsi al sito CPPLSDPU, scaricare in maniera riservata, sempre mediante Tor o Tor2Web, il Tulip, e dopo averlo esaminato potrà scaricare il relativo documento, ed ovviamente decidere se utilizzarne o meno i contenuti.

Tramite Tor sia il Whisteblower che l'Administrator potranno esaminare in ogni momento lo stato del Tulip, e sapere se è stato letto e se il documento allegato è stato scaricato per ogni Target. In aggiunta a questo l'Administrator può esaminare tutti i Tulip creati sul suo sito ed eventualmente cancellarli in qualsiasi momento.

Il Tulip non è eterno, ma ad un certo punto "muore" automaticamente. Come un tulipano, muore alla fine della bella stagione (una data di scadenza decisa al momento della creazione) o quando tutti i petali sono stati staccati (tutti i Target l'hanno scaricato).

È disponibile una demo concettuale della realizzazione ed utilizzo di un sito Globaleaks.

Il gruppo di sviluppatori di Globaleaks mette anche a disposizione alcune interessanti risorse, tra cui la LeakDirectory, un wiki contenente un elenco veramente impressionante di tutte le risorse per la public disclosure passate e presenti, tra cui siti, documenti, legislazione ed organizzazioni interessate.

La data di rilascio della prima release utilizzabile di Globaleaks non è stata ancora comunicata, ma è imminente.
Una introduzione al progetto Globaleaks è contenuta in queste slide.

Chi volesse partecipare in prima persona a questa avventura puo diventare Random Globaleaks Contributor collaborando con la comunità tramite il sito ed il wiki. Maggiori informazioni sono disponibili in questa pagina.

Stay tuned.

Figure 3:

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on February 22, 2023.

Canonical link

Exported from Medium on August 27, 2025.